Guide de Formation

Sécurisation des Services PaaS avec Azure Private Link

Projet : DataSafe Corp
Auteur : NGUYEN Minh Kha
Date : 03/07/2025

Table des matières

---

1. Introduction : Le problème de la sécurité des services PaaS

Les points de terminaison publics par défaut Par défaut, la plupart des services de type "Platform-as-a-Service" (PaaS) sur Azure, comme Azure Storage, Azure SQL Database ou Azure Key Vault, sont conçus pour être accessibles via des points de terminaison publics. Cela signifie que leur URL (par exemple, `mondatasafecorp.blob.core.windows.net`) se résout en une adresse IP publique, accessible depuis n'importe où sur Internet.

Bien que cet accès soit protégé par des mécanismes d'authentification (clés d'accès, jetons SAS, etc.), le point de terminaison lui-même reste exposé.

Les risques associés Cette exposition sur le réseau Internet public, même si elle est contrôlée, présente plusieurs risques fondamentaux pour une organisation

comme DataSafe Corp qui manipule des données sensibles :

- **Surface d'attaque élargie :** Le service est directement visible et accessible depuis Internet, ce qui en fait une cible potentielle pour des attaques par force brute, des recherches de vulnérabilités ou des attaques par déni de service (DDoS).
- **Risque d'exfiltration de données :** Une clé d'accès ou un jeton qui fuite (par exemple, via un code source publié par erreur sur un dépôt public) peut permettre à un attaquant d'accéder directement aux données depuis n'importe où dans le monde.
- **Non-conformité réglementaire :** De nombreuses réglementations (comme le RGPD) exigent que l'accès aux données sensibles soit strictement contrôlé et limité à des réseaux privés et de confiance.

L'objectif est donc de supprimer complètement cette exposition publique et de s'assurer que nos services PaaS ne sont accessibles que depuis notre réseau interne sécurisé.

2. Azure Private Link et Private Endpoint : La solution

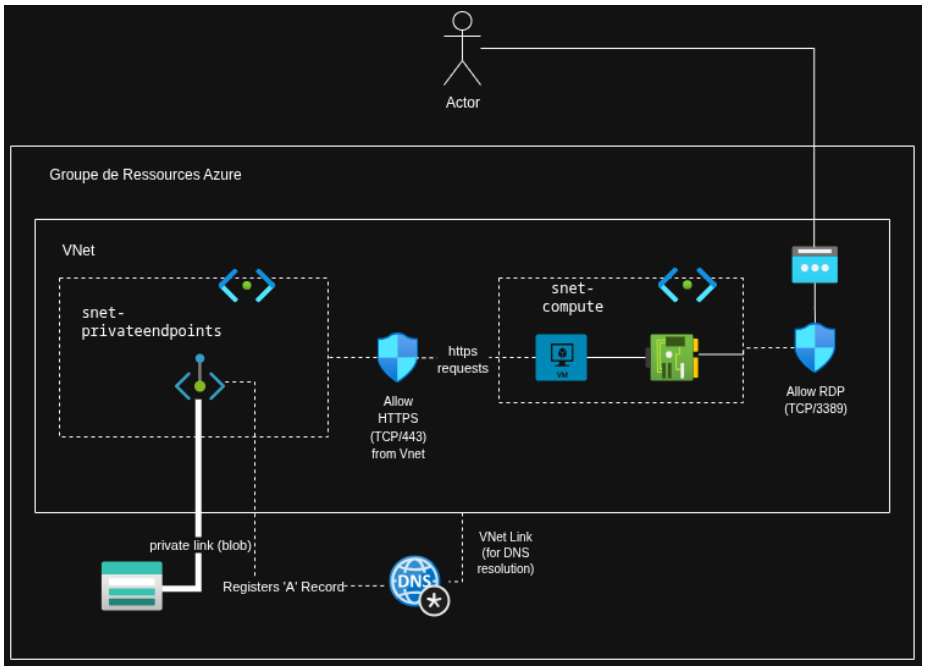
Qu'est-ce qu'Azure Private Link ? Azure Private Link est le service global qui permet de consommer des services PaaS Azure (ou même des services hébergés par des partenaires) de manière privée, sans jamais exposer le trafic à l'Internet public. Le trafic entre votre réseau virtuel et le service transite entièrement par le réseau principal (backbone) de Microsoft.

Le Private Endpoint : une interface réseau privée pour vos services Pour utiliser Private Link, on crée un **Private Endpoint** (Point de terminaison privé).

Un Private Endpoint est une **interface réseau (NIC)** qui dispose d'une **adresse IP privée** issue de votre propre réseau virtuel (VNet). Cette interface réseau vous connecte de manière privée et sécurisée à un service PaaS. En d'autres termes, au lieu que votre service PaaS soit "quelque part sur Internet", le Private Endpoint **l'intègre directement dans votre réseau privé**.

Les principaux avantages sont : * **Sécurité renforcée :** Le trafic ne quitte jamais votre réseau virtuel et le réseau Microsoft pour atteindre le service. * **Protection contre l'exfiltration de données :** Le Private Endpoint est mappé à une ressource spécifique (ex: un compte de stockage précis) et non à tout le service Azure Storage. Il est donc beaucoup plus difficile pour un acteur malveillant d'utiliser cette connexion pour atteindre un autre compte de stockage. * **Connectivité simplifiée :** L'accès depuis des réseaux sur site (via VPN ou ExpressRoute) et des réseaux virtuels appairés est possible de manière native.

Architecture de notre solution Dans le cadre du projet DataSafe Corp, nous avons déployé l'architecture sécurisée suivante :



[Schéma Réseau]

Ce schéma illustre comment notre machine virtuelle (VM), située dans le subnet "compute", accède au compte de stockage. Au lieu de sortir sur Internet, la communication est redirigée vers le Private Endpoint, situé dans son propre subnet dédié, qui établit ensuite une connexion sécurisée vers le service de stockage sur le réseau principal de Microsoft.

3. L'importance du DNS : Comment ça marche ?

Faire entrer un service PaaS dans notre VNet via une IP privée est une chose, mais comment s'assurer que nos applications continuent de l'utiliser de manière transparente, sans changer les URLs de connexion ? C'est là que le DNS entre en jeu.

Le rôle de la Private DNS Zone Lorsque vous utilisez un Private Endpoint, il est essentiel de configurer correctement le DNS pour que le nom de domaine public du service (ex: `mondatasafecorp.blob.core.windows.net`) se résolve non pas vers son IP publique, mais vers l'**IP privée** de votre Private Endpoint.

Pour ce faire, nous utilisons une **Azure Private DNS Zone**. Il s'agit d'un service DNS qui ne fonctionne qu'à l'intérieur de vos réseaux virtuels. En liant cette zone DNS privée à notre VNet, nous pouvons remplacer la résolution DNS publique par notre propre configuration.

Le processus de résolution de nom Voici le déroulement d'une requête lorsque la configuration est en place :

1. **Requête DNS :** Une application sur la VM dans notre VNet tente de se connecter à `mondatasafecorp.blob.core.windows.net`. Elle effectue donc une requête DNS pour ce nom.
2. **Redirection vers la Zone Privée :** Comme le VNet est lié à notre Private DNS Zone (`privatelink.blob.core.windows.net`), le service DNS d'Azure ne contacte pas les serveurs DNS publics. Il redirige la requête vers notre zone privée.
3. **Résolution en IP Privée :** La Private DNS Zone contient un enregistrement de type 'A' qui mappe `mondatasafecorp` à l'adresse IP privée du Private Endpoint (ex: `10.10.1.4`).
4. **Connexion sécurisée :** La VM reçoit cette IP privée et établit une connexion TCP directement avec le Private Endpoint à l'intérieur du VNet. La communication est sécurisée et privée.

À l'inverse, une machine en dehors du VNet qui effectue la même requête DNS recevra l'adresse IP publique du service, mais la connexion sera bloquée par le pare-feu du compte de stockage, qui n'autorise plus aucun accès public.

4. Notre implémentation : Le projet DataSafe Corp

Déploiement avec Terraform Pour garantir un déploiement fiable, reproductible et standardisé, nous avons utilisé l'approche d'Infrastructure-as-Code (IaC) avec Terraform. Notre code est structuré en modules (networking, storage, compute) pour une meilleure maintenabilité.

Analyse des ressources clés Voici les extraits de code Terraform essentiels qui mettent en œuvre cette architecture sécurisée.

1. Désactiver l'accès public au Stockage (fichier `locals.tf`) Cette configuration est le point de départ de notre sécurisation. Nous indiquons explicitement que le compte de stockage ne doit accepter aucune connexion depuis le réseau public.

```
storage_config = {
  # ... autres configurations
  public_network_access_enabled   = false
  # ...
}
```

2. Création du Private Endpoint (fichier `modules/storage/main.tf`) Ce bloc de code crée l'interface réseau privée. Il la place dans le subnet dédié et la connecte à notre compte de stockage, en ciblant spécifiquement le sous-service `blob`.

```
resource "azurerm_private_endpoint" "main" {
  for_each = var.private_endpoints
```

```
  name                = "pep-${var.storage_config.name}-${each.key}"
  location            = var.location
  resource_group_name = var.resource_group_name
  subnet_id           = var.subnet_id

  private_service_connection {
    name                           = "psc-${var.storage_config.name}-${each.key}"
    private_connection_resource_id = azurerm_storage_account.main.id
    subresource_names              = each.value.subresource_names
    is_manual_connection           = false
  }
}
```

3. Liaison à la Private DNS Zone (fichier `modules/storage/main.tf`)
Ce bloc `private_dns_zone_group` associe le Private Endpoint à la zone DNS privée. C'est ce qui permet de créer automatiquement l'enregistrement 'A' qui fait le lien entre le nom FQDN du service et l'IP privée du Private Endpoint.

```
  # ... dans la ressource azurerm_private_endpoint ...
  dynamic "private_dns_zone_group" {
    for_each = contains(keys(var.private_dns_zone_ids), each.value.private_dns_zone) ? [1] :

    content {
      name                 = "pdzg-${each.key}"
      private_dns_zone_ids = [var.private_dns_zone_ids[each.value.private_dns_zone]]
    }
  }
```

4. Liaison de la Zone DNS au VNet (fichier `modules/networking/main.tf`)
Enfin, cette ressource cruciale lie la zone DNS privée à notre réseau virtuel, activant ainsi le mécanisme de résolution de noms privé pour toutes les ressources du VNet.

```
resource "azurerm_private_dns_zone_virtual_network_link" "main" {
  count = var.enable_private_dns_zone ? 1 : 0

  name                  = "vnet-link-${var.vnet_name}"
  resource_group_name   = var.resource_group_name
  private_dns_zone_name = azurerm_private_dns_zone.main[0].name
  virtual_network_id    = azurerm_virtual_network.main.id
  registration_enabled  = false
}
```

5. Bonnes pratiques et sécurité

La mise en place de Private Link est une étape majeure, mais elle doit être complétée par d'autres bonnes pratiques pour assurer une sécurité maximale.

Règles d'or pour une configuration robuste

- **Toujours désactiver l'accès public :** La première étape doit systématiquement être de désactiver la propriété `public_network_access_enabled` sur la ressource PaaS.
- **Utiliser des subnets dédiés :** Bien que ce ne soit pas une obligation technique, dédier un subnet aux Private Endpoints est une bonne pratique. Cela permet d'appliquer des politiques de sécurité spécifiques à ce subnet sans impacter les autres ressources comme les VMs.
- **Contrôle d'accès avec les NSG :** Par défaut, un subnet ne peut pas avoir de Network Security Group (NSG) si des Private Endpoints s'y trouvent. Cependant, il est possible (et recommandé) d'activer les "politiques réseau" sur le subnet. Cela permet d'associer un NSG et de filtrer le trafic à destination du Private Endpoint, offrant ainsi une couche de défense en profondeur. Par exemple, on peut s'assurer que seules les VMs du subnet "compute" peuvent communiquer avec le Private Endpoint sur le port 443.
- **Utiliser une zone DNS privée par type de service :** Évitez de regrouper les enregistrements de différents types de services (ex: blob, table, sql) dans la même zone DNS pour éviter les conflits.

Monitoring et audit La sécurité ne s'arrête pas à la configuration. Il est crucial de surveiller qui accède à vos ressources : * **Logs de diagnostic :** Activez les logs de diagnostic sur le compte de stockage et envoyez-les à un espace de travail Log Analytics. Cela vous permettra de tracer chaque tentative d'accès, qu'elle soit réussie ou non. * **Azure Monitor pour les Private Endpoints :** Le Private Link Center dans Azure Monitor fournit des métriques sur le trafic entrant et sortant du Private Endpoint. * **NSG Flow Logs :** Si vous avez activé les politiques réseau et déployé un NSG, les journaux de flux (Flow Logs) vous donneront une visibilité détaillée sur le trafic accepté et refusé au niveau du subnet.

6. Annexe

Glossaire

- **PaaS (Platform-as-a-Service) :** Modèle de cloud computing où un fournisseur tiers livre des outils matériels et logiciels aux utilisateurs sur Internet. Exemples : Azure Storage, Azure SQL.
- **VNet (Virtual Network) :** Un réseau privé et isolé au sein d'Azure.
- **Private Link :** Le service Azure qui permet une connectivité privée des réseaux virtuels aux services Azure.
- **Private Endpoint (Point de terminaison privé) :** Une interface réseau avec une IP privée dans votre VNet qui se connecte à un service Azure compatible Private Link.
- **Private DNS Zone :** Un service qui fournit une résolution de noms de domaine fiable et sécurisée pour un réseau virtuel, sans passer par Internet.

- **NSG (Network Security Group) :** Un pare-feu de base qui contient une liste de règles de sécurité autorisant ou refusant le trafic réseau vers les ressources.

Références

- **Documentation officielle Azure Private Link :** https://docs.microsoft.com/azure/private-link/
- **Qu'est-ce qu'un Private Endpoint ? :** https://docs.microsoft.com/azure/private-link/private-endpoint-overview
- **Configuration DNS des Private Endpoints :** https://docs.microsoft.com/azure/private-link/private-endpoint-dns
- **Provider Terraform - `azurerm_private_endpoint` :** https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/private_endpoint
- **Provider Terraform - `azurerm_private_dns_zone_virtual_network_link` :** https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/private_dns_zone_virtual_network_link